Rising Financial Crime Risks in Digital Payments

Maintain user satisfaction while prioritizing risk identification and management to meet the demands of evolving regulatory focus

Financial technology (FinTech) has propelled the speed at which payments are made, increased the reach of digital payments across borders, and expanded the accessibility of financial services to users worldwide. In 2022, the global digital payment market size was valued at **USD 81.03 billion**, with global digital payments valued at over USD 8 trillion, and the market size is only expected to continue, at an annual **growth rate of around 20% in the next seven (7) years**[1]. There is no doubt that digital payment services are becoming more attractive than traditional financial services. Digital payments occur in real-time and payment services are generally free to use, whereas traditional banking channels can take days to complete, may require a fee to process a transaction, and may involve bank intermediaries. In efforts to remain competitive, improve customer satisfaction, and drive business, companies are focusing more and more on digital payment innovations.

Behind the scenes, bad actors or criminals are keeping up with the pace and advances in FinTech, often actively developing new strategies to exploit digital payment products and services to hide the origins of their criminal activities and take advantage of vulnerabilities and weaknesses in organizations' compliance frameworks. The rise of digital payments has increased the potential for financial crime risks (namely fraud, money laundering, terrorist financing, and sanctions risks). As such, FinTech companies are constantly focused on balancing between the need to maintain user satisfaction and prioritizing the identification and management of increased financial crime risks to meet the demands of evolving regulatory focus.

[1] Source: Grand View Research, Digital Payment Market Size, Share & Trends Analysis Report By Deployment (Cloud, On-premise), By Solution (Payment Gateway, Payment Processing), By Mode of Payment, By Enterprise Size, By End-use, And Segment Forecasts, 2023 - 2030

Top Financial Crime Trends and Typologies

One unavoidable downfall resulting from the growth in digital payments is the increased risk in financial crime activities. Criminals are increasingly engaging in sophisticated schemes in efforts to obtain and/or launder illicit funds. Below are some of the most common trends and typologies that we see impacting the payments industry today:

Micro-Structuring

Bad actors may potentially launder illicit funds by splitting up payments into multiple smaller transfers to evade detection. A potential indicator of micro-structuring could entail frequent incoming and/or outgoing activities in an account that is in volumes or amounts that is unusual especially compared to other similar customers.

Identity Theft

In this case, a criminal steals a user's banking or credit card information via data breaches/ malware/fishing or scam calls and uses the stolen information to pay for goods and services through e-commerce platforms or transfer funds to other accounts via online payments platforms (e.g., Peer-to-Peer (P2P) payments).

Use of Third Parties/Money Mules

In order to disguise their identity or the true origin of funds, criminals may leverage money mules or a network of associates to transfer illicit funds to/from multiple different accounts, often to/from different jurisdictions. Knowingly, criminals can exploit weaknesses in financial crimes compliance programs that do not have proper controls to identify money laundering networks.

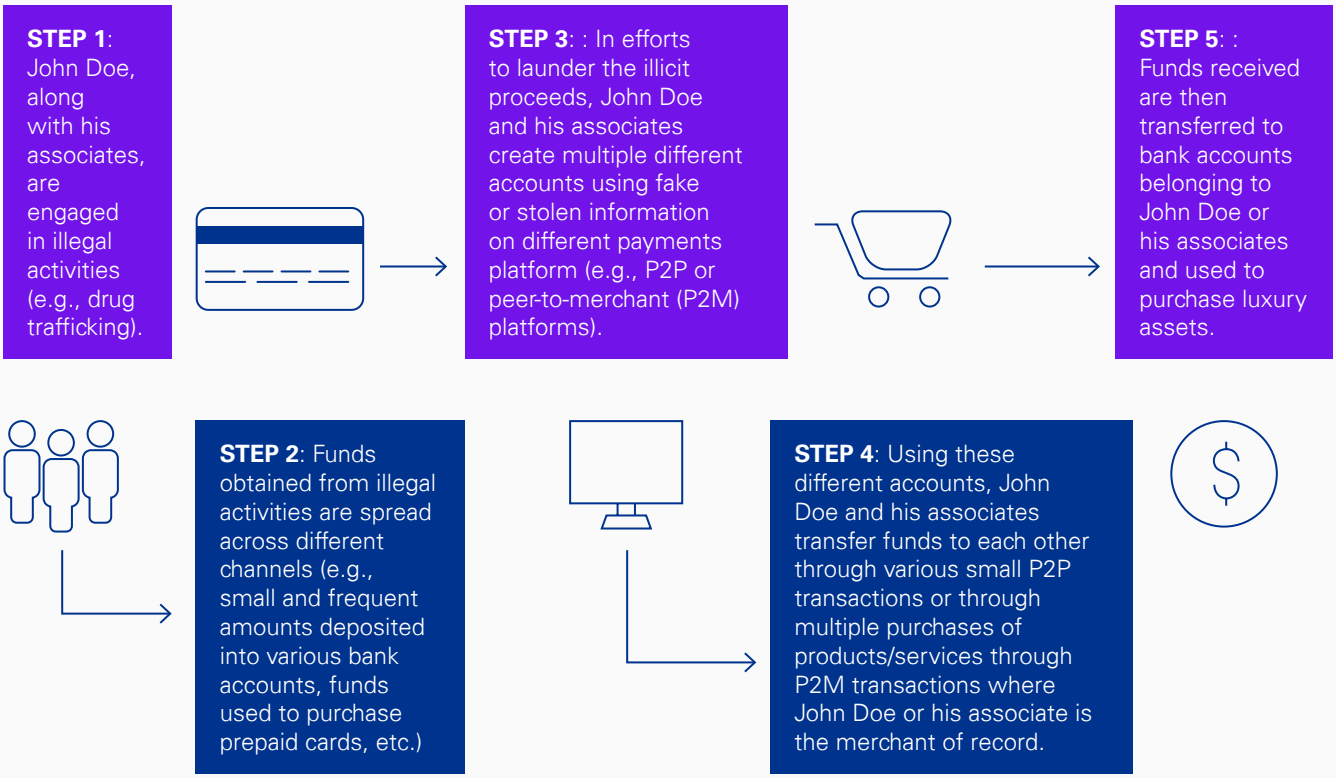

Figure 1: Example of a money laundering and fraud scheme

Managing Financial Crime Risks

Managing financial crime risks in today's day and age may feel like a daunting task. As digital payment providers consider their approach in managing financial crime risks, companies should focus in on the following strategies:

- **Focus on strategic effectiveness rather than "check-the-box" compliance**: As criminals continue to find new and innovative ways to further their illicit activities, check-the-box approaches to compliance may not be the most effective approach to prevent financial crime exploitation. Companies should focus on outcomes instead of outputs in its compliance programs. This includes implementing a data-driven continuous monitoring approach in its overall risk management strategy, leveraging the outcomes to drive the company's priorities, and focus its efforts on aligning its compliance programs to those priorities.
- **Move to Perpetual Know Your Customer (P-KYC) Processes**: Companies need to re-imagine the way KYC is being conducted and invest in technology that enables KYC processes to be automated. This includes focusing efforts on improving the quality of data that is being collected to allow companies to better understand their customer's risk profile and move away from traditional customer periodic review processes to real-time monitoring that is powered by technology. This will allow for more value-added output, reduction in operational costs, and a significant reduction in the need for human intervention.
- **Invest in next-generation financial crime detection**: Rather than investing in headcount to clear high volume of alerts, many of which may be false positives, companies should instead focus its efforts on deploying machine learning and artificial intelligence to their financial crime detection process with the end goal of identifying higher value alerts.

Whether your company is looking for guidance on how to approach your compliance programs or looking to transform your entire compliance strategy, the KPMG Forensic team can provide insights and guidance along the way. Our team has the experience, skillsets and tools to help you create a best-in-class compliance program[2].

[2] The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Contact us

Matthieu Chabelard
Principal, Advisory, Forensic
KPMG LLP
T: 917-513-4152
E: mchabelard@kpmg.com

Ada Tsai
Director Advisory, Forensic
KPMG LLP
T: 917-592-2120
E: adatsai@kpmg.com

Contributor

Michelle Nolasco
Manager, Advisory, Forensic
KPMG LLP

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia